REMARKS

Claims 1 - 3, 6 - 11, 20, and 23 - 41 are pending. Claims 1 - 3, 6, 9 - 12, 15 - 20, and 23 - 27 have been amended. Claims 4 - 5, 12 - 19, and 21 - 22 have been cancelled. Claims 28 - 41 have been added. No new matter has been introduced. Reexamination and reconsideration of the application are respectfully requested.

In the December 19, 2003 Office Action, the Examiner rejected claims 1 - 10, 12 - 18, and 20 - 26 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,360,269 to Mamros et al. (the Mamros reference). The Examiner rejected claims 11, 19, and 27 under 35 U.S.C. § 103(a) as being unpatentable over the Mamros reference. These rejections are respectfully traversed.

Embodiments of the present invention are directed to a method of providing security mechanisms for securing traffic communication between a server system and a client system. The method includes detecting whether the client system is in operational state and executes first key exchange processes between the server system and the client system when the client system is in the operational state. The client system stores the results of the first key exchange processes. Stored results are inhibited from being updated until a successful execution of a second set of key exchange processes between the server system and the client system. If the second set of key exchange processes is successful, the stored results are updated with the results from the second set of key exchanges.

Claim 1, as amended, recites:

> A computer network comprising:
>
> a server system;

a client system;

logic for detecting whether the client system is in an operational state;

logic for executing a first key exchange process to produce results;

a storage device at the client system for storing the results of the first key exchange process;

logic for inhibiting the stored results of the key exchange from being updated until a successful execution of a second key exchange process between the server system and the client system;

logic for updating the stored results of the first key exchange process if execution of the second key exchange process is successful; and and

logic to secure traffic communication between the client system and the server system utilizing the results of the first key exchange process if the second set of key exchange processes is not successful because the client system becomes non-operational.

The Mamros reference is directed to a method and apparatus for determining the reachability of a remote computer through a secured communications link through the Internet. The Examiner states that the Mamros reference discloses "logic for inhibiting the stored results of the key exchange from being updated until a successful execution of another set of key exchange processes between the server system and the client system" at col. 6, lines 52 - 67 and col. 7, lines 1 - 17. *(Dec. 19 Office Action, page 2).* At col. 6, line 52 - col. 7, line 17, the Mamros reference discloses that the results which occur when a connection between a modem 013 and an ISP 121 has been dropped, i.e., 1) the user may not be able to login until the previous security association has been torn down if only one secured link to the LAN is available; or 2) under ISAKMP / Oakley, the security association is not torn down until the above timeout exception occurs.

This is not the same as a computer network including a server system, a client system, logic for executing a first key exchange process to produce results;
a storage device at the client system for storing the results of the first key exchange process, and **logic for inhibiting the stored results of the first key exchange process from being updated until a successful execution of a second key exchange process between the server system and the client system**. The Mamros reference does not discuss or disclose where the keys are stored after the key exchange. In addition, assuming, *arguendo*, that keys are stored after the first key exchange process, there is no discussion of any logic or structure that inhibits stored keys information from being updated. Accordingly, applicants respectfully submit that independent claim 1, as amended, distinguishes over the Mamros reference.

Independent claim 1, as amended, further distinguishes over the Mamros reference. The Mamros reference does not disclose, teach, or suggest, a computer network including a including a server system, a client system, logic for executing a first key exchange process to produce results; a storage device at the client system for storing the results of the first key exchange process, and **logic to secure traffic communication between the client system and the server system utilizing the results of the first key exchange process if the second key exchange process is not successful.**

Instead, the Mamros reference discloses that "in the event that a remote computer or box fails to respond to a re-key request under the ISAKMP/Oakley protocol, it is assumed that the remote computer box is no longer reachable and the protected Internet communication and associated security association under the ISAKMP / Oakley protocol is torn down." *(Mamros, col. 6, lines 36 - 51)*.

This is not the same as logic for utilizing the **results of the first key exchange process to secure traffic communication between the client system and the server system utilizing the results of the first key exchange process if the second key exchange process is not successful because the client system becomes non-operational.** If the communication and security association is torn down, as the Mamros reference discloses, it is impossible to utilize the results of the first key exchange processes because no communication is taking place. Accordingly, applicants respectfully submit that independent claim 1, as amended, further distinguishes over the Mamros reference.

Independent claims 20, 32, and 38, recite similar limitations to independent claim 1, as amended. Accordingly, applicants respectfully submit that independent claims 20, 32, and 38 distinguish over the Mamros reference for similar reasons to those discussed above in regard to independent claim 1, as amended.

Dependent claims 2 - 11, 21 - 31, 33 - 37, and 39 - 41 depend, directly or indirectly, from independent claims 1, 20, 32, and 38. Accordingly, applicants respectfully submit that dependent claims 2 - 11, 21 - 31, 33 - 37, and 39 -41 all distinguish over the Mamros reference for the same reasons as those discussed above in regard to independent claims 1, 20, 32, and 38.

Dependent claim 28 further distinguishes over the Mamros reference.

Dependent claim 28 recites:

> The method of claim 20, wherein using the stored results to secure the traffic further includes **transmitting management Internet Protocol-based packets from the server system to the client system if the client system is determined to be non-operational to perform diagnostic operations on the client system**.

The Mamros reference does not disclose, teach, or suggest the method of independent claim 28. The Mamros reference discloses that "[i]n the event that that a remote computer or box fails to respond to a re-key request under the ISAKMP/Oakley protocol, it is assumed that the remote computer box is no longer reachable and the protected Internet communications link and associated security association under the ISAKMP/Oakley protocol is torn down." *(Col. 6, lines 42 - 51)*. The Mamros reference also discloses that if there has not been any communication between the local and remote systems for a specified period of time, then a protected keepalive message is sent from the local box to the first box. If the remote system transmits a protected acknowledgment in response to the keepalive message, then the system continues to transmit securely. However, if no protected acknowledgment is received then secured communications between local and remote boxes is discontinued. *(See Fig. 4, col. 8, line 23 - col. 9, line 20)*.

This is not the same as a method of providing security mechanisms for securing traffic communication between a server system and a client system wherein using the stored results to secure the traffic further includes **transmitting management Internet**

Protocol-based packets from the server system to the client system if the client system is determined to be non-operational to perform diagnostic operations on the client system. It is not the same because the Mamros reference does not discuss transmitting management IP-based packets at all. In addition, if the client system, i.e., remote system, is determined to be non-operational, the local system in the Mamros reference transmits a keepalive message to the local system to attempt to receive a protected acknowledgement from the remote system and if an acknowledgment is not received, the Mamros reference terminates the secured communication. This is in contrast to transmitting packets from the server system to the client system **if the client system is determined to be non-operational in order to perform diagnostic operations, as recited in dependent claim 28,** because the Mamros reference has terminated the transmission of packets. Accordingly, applicants respectfully submit that dependent claim 28 further distinguishes over the Mamros reference.

Dependent claim 37 recites similar limitations to dependent claim 28. Accordingly, applicants respectfully submit that dependent claim 37 distinguishes over the Mamros reference for similar reasons as discussed above in regard to dependent claim 28.

Dependent claim 29 further distinguishes over the Mamros reference. Dependent claim 29 recites:

> The method of claim 28, wherein the transmission of management IP-based protocol packets **causes the client system to re-boot**.

The Mamros reference does not disclose, teach, or suggest the method of claim 28. As noted above, the Mamros reference does not disclose or teach the transmission of management IP-based protocol packets. Because the Mamros reference does not disclose or teach the transmission of management IP-based protocol packets, it is impossible for the management IP based protocol packets to cause the client system to reboot. In additional, there is no discussion of the Mamros computers sending communications to cause the other systems to reboot. Accordingly, applicants respectfully submit that dependent claim 29 further distinguishes over the Mamros reference.

Dependent claim 30 further distinguishes over the Mamros reference. Dependent claim 30 recites:

> The method of claim 29, wherein the management IP-based protocol packets are **remote management and control protocol (RCMP) packets.**

The Mamros references does not disclose, teach, or suggest the method of claim 30. The Mamros reference does not mention or disclose management IP-based protocol packets, generally, or remote management and control protocol (RCMP) packets, specifically. Accordingly, applicants respectfully submit that dependent claim 30 distinguishes over the Mamros reference.

Dependent claim 31 further distinguishes over the Mamros reference. Dependent claim 31 recites:

> The network system of claim 1, further including a plurality of client systems coupled to the server system, each of the plurality of client systems including a security parameter, wherein **the server system includes a non-volatile storage for storing the security parameter for**

each of the plurality of client systems.

The Mamros reference does not disclose, teach, or suggest the network system of claim 31. The Mamros reference does not specifically discuss the storage of keys within the computer systems 10 , or remote systems 113 and117. The Mamros reference does disclose that the computer systems 101, 113, and 117 may include mass memory, DRAM, and SRAM. *(Col. 4, lines 1 - 35).* However, there is no specific discussion of storing the keys within the mass memory, DRAM and SRAM. The Examiner states that storage of the results of the key exchange process is inherent in ISAKMP, because the key is carried in the channel. *(Office Action, page 2)*. Applicants respectfully disagree with the assumption that because the key is carried in a channel, that inherently there is storage for storing the results of the key exchange processes. Assuming, *arguendo*, that the Mamros reference does disclose the storage of keys, the Mamros reference does not disclose or discuss **the server system including a non-volatile storage for storing the security parameter for each of the plurality of client systems.** Accordingly, applicants respectfully submit that dependent claim 31 distinguishes over the Mamros reference.

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

Applicants believe that the claims are in condition for allowance, and a favorable action is respectfully requested. If for any reason the Examiner finds the application other than in condition for allowance, the Examiner is requested to call either of the undersigned attorneys at the Los Angeles telephone number (213) 488-7100 to discuss the steps necessary for placing the application in condition for allowance should the Examiner believe that such a telephone conference would advance prosecution of the application.

Respectfully submitted,

PILLSBURY WINTHROP LLP

Date: March 18, 2004

By:
Mark R. Kendrick
Registration No. 48,468
Attorney for Applicant(s)

Date: March 18, 2004

By:
Roger R. Wise
Registration No. 31,204
Attorney For Applicant(s)

725 South Figueroa Street, Suite 2800
Los Angeles, CA 90017-5406
Telephone: (213) 488-7100
Facsimile: (213) 629-1033